REMARKS

Claims 1-33, 35, 37, 38 41 and 42 are pending in this application. Claims 15, 35 and 37 have been amended. Claims 1-14 and 30-34 have been canceled.

Claims 1-33 and 35, 37, 38, 41 and 42 were rejected under 35 USC §103(a) as being unpatentable over Carter (U.S. Patent No. 5,787,175) in view of Follendore, III (U.S. Patent No. 6,011,847).

Independent Claim 15, as amended, claims a secure content object, comprising: an encrypted electronic document having been encrypted with a document encryption key, wherein access to the electronic document is available to a first set of authorized users; an encrypted header comprising information pertaining to the electronic document; a first multi-key encryption table for use in a multi-key encryption method associated with the electronic document, the first table comprising at least one multi-key component associated with each authorized user in the first set and a plurality of dummy encryption components, wherein the multi-key encryption table includes no information that may identify a user or the electronic document; a plurality of annotations generated by an annotation author, the plurality of annotations having been encrypted with an annotation encryption key, wherein access to the plurality of annotations is available to the authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations; a second multi-key encryption table for use in a multi-key encryption method associated with the plurality of annotations, the second table comprising at least one multi-key component associated with each authorized annotation user; and a user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic document, for inputting the user authorization to a decryption engine using the multi-key encryption method for combining the user authorization with each of the multi-key components in the first multi-key encryption key table to decrypt the encrypted header, and for combining the user authorization with each of the stored multi-key components in the second multi-key encryption key table to decrypt an annotation, wherein upon a valid decryption of the annotation indicates the correct annotation encryption key has been found and

the user is an authorized annotation user; and upon a valid decryption of the encrypted header, for enabling decryption of the portion of the encrypted electronic document.

The secure content object enables users to create annotations pertaining to an existing electronic document and to limit access to those annotations to certain users and providing encrypted security for the annotations. The secure content object may be used in those instances when multiple authors may wish to make annotations or comments to a common electronic document and control access (and knowledge of) their annotations among other users. For example, the original electronic document may have no restrictions on viewing (all users may view it), so it is not encrypted. One or more users/authors (including the original author) may wish to make annotations or comments to the electronic document. Each annotation author may wish to limit access to one or more of the annotations. Each such annotation may be encrypted and access limited to certain users.

Independent Claim 35, as amended, claims a method for creating a document with secure annotations, comprising: providing an electronic document, wherein access to the electronic document is available to a first set of users; responsive to a first user from the first set of users, generating a plurality of annotations pertaining to the electronic document using the document language and associating the plurality of annotations with the first user; designating which users in the first set of users are authorized users have access to the plurality of annotations; encrypting each annotation using an annotation encryption key associated with the first user generating the particular annotation, wherein access to an encrypted annotation is available to authorized users having access to the respective annotation encryption key; for each annotation encryption key: generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component associated with each authorized user having been designated by the first user as having access to the annotation; providing a user interface for enabling a user to input a user authorization for access to at least a portion of an encrypted annotation; wherein, responsive to an input user authorization, combining the input user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found; concatenating the plurality of encrypted annotations

in a second electronic document; and merging the second electronic document and the encrypted electronic document into a third electronic document such that access to the encrypted electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to authorized users.

1) Carter teaches that each authorized member has access to the entire document.

Carter teaches a method and apparatus for collaborative document control. In Carter, a document 90 includes an encrypted data portion 94 and a header portion which includes a plurality of member definitions 96. Each member definition 96 includes an unencrypted member identifier 98, an encrypted document key 100 and an optional encrypted message digest or hash 102 (see Figs. 4, 5 of Carter). The member definitions 96 define a collaborative group of computer system users which have access to the data portion 94 of the work group document 90 (col. 12, lines 29-32). Figs. 2-6 and 9 of Carter illustrate a method for restricting access to the information in the data portion 95 of the work group document 90 so that members of the collaborative group have access and others do not (col. 15, lines 63-67). Carter does not teach or suggest allowing users in the collaborative group to add annotations the document without granting access to all members of the collaborative group. Carter does not teach or suggest a secure content object in which, in part, access to the plurality of annotations is available to the authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations.

2) Carter's encrypted message digest is not the same as an encrypted annotation.

Carter teaches an encrypted message digest 102 which provides a member of the collaborative group the ability to collaborative sign a version of the document. An encrypted message digest is used to control attribution of a document. Figs. 2-6 and 10 of Carter illustrate a method for collaboratively signing a document 90. Collaborative signatures control the attribution of a given version of the work group document 90 to one or more members of the collaborative group (col. 17, lines 28-33). As best as Carter is understood, access and decryption of a particular member's member digest is available to all members of the collaborative group. It would appear to be important to the collaborative group to know which members claimed attribution to the collaborative document 90 and to which version.

In contrast, in Applicant's secure content object, a user which creates a plurality of annotations can control which of the users having access to the document can have access to his/her annotations. In Applicant's secure content object, access to the plurality of annotations is available to the authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations.

3. Follendore III is concerned with controlling keys, not with controlling access to documents and annotations associated with the document.

Follendore III is concerned with the need for a key management system which will keep track of the keys that are used with a particular message, but will also maintain the justification for the use of that key and the justification for the different categories of personnel access and the criteria used for selecting the communication system (col. 2, lines 20-26). Follendore III teaches managing encryption keys through the use of labels appended to a message (col. 5, lines 34-38). Although different keys may be used to encrypt the labels appended to the message, it does not appear that any user has access to the encrypted labels. Fig. 2 of Follendore III shows a decryption process in which a user inputs a pass phrase 212. The pass phrase is used to decrypt the labels 232 which results in a file key input into a run algorithm 236 which produces a decrypted file 242. The user does not have access to the decrypted file key (other than to receive the benefit of it having been used to decrypt the message).

4. Follendore III teaches that each authorized member has access to the entire document.

As best Follendore III is understood, Fig. 2 of Follendore III shows a user having entered a valid pass phrase having access to the entire decrypted document. As best Follendore III is understood, no authorized user has access to the decrypted labels. In Applicant's secure content object, access to the plurality of annotations is available to the authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations.

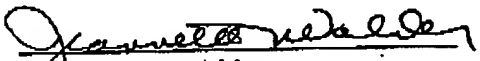
Independent Claims 15 and 35 are believed to be allowable. Since Claims 16-29 depend from Claim 15 and Claims 37, 38, 41 and 42 depend from Claim 35, they are also believed to be

allowable. Claims 15-29 and 35, 37, 38, 41 and 42 are believed to be in condition for allowance.

No additional fee is believed to be required for this amendment; however, the undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025.

Reconsideration of this application and allowance thereof are earnestly solicited. In the event the Examiner considers a personal contact advantageous to the disposition of this case, the Examiner is requested to call the undersigned Attorney for Applicant, Jeannette Walder.

Respectfully submitted,



Jeannette M. Walder
Attorney for Applicant
Registration No. 30,698
Telephone: 714 565-1700

Xerox Corporation
Santa Ana, California
Date: May 23, 2005